

CANCELLATIONS BETWEEN KLOOSTERMAN SUMS MODULO A PRIME POWER WITH PRIME ARGUMENTS

KUI LIU, IGOR E. SHPARLINSKI, AND TIANPING ZHANG

ABSTRACT. We obtain a nontrivial bound for cancellations between the Kloosterman sums modulo a large prime power with a prime argument running over very short interval, which in turn is based on a new estimate on bilinear sums of Kloosterman sums. These results are analogues of those obtained by various authors for Kloosterman sums modulo a prime. However the underlying technique is different and allows us to obtain nontrivial results starting from much shorter ranges.

1. INTRODUCTION

1.1. Background and motivation. For an integer $q \geq 1$ and arbitrary integers m and n , we define the Kloosterman sums

$$\mathcal{K}(m, n; q) = \frac{1}{q^{1/2}} \sum_{b \bmod q}^* e\left(\frac{mb + n\bar{b}}{q}\right),$$

where \sum^* means summing over reduced residue classes, \bar{b} is given by $b\bar{b} \equiv 1 \pmod{q}$ and for a real x we denote

$$e(x) = e^{2\pi i x}.$$

First we recall that the Weil bound, see [5, Corollary 11.12], yields the estimate

$$(1.1) \quad |\mathcal{K}(m, n; q)| \leq \sqrt{\gcd(m, n, q)} q^{o(1)},$$

which gives an optimal bound on individual Kloosterman sums. So any further progress in their applications is possible only via studying their finer structure and possible cancellations in various families of these sums.

Indeed, starting from the groundbreaking results of Kuznetsov [9] towards the Linnik conjecture [10] on cancellations between Kloosterman sums, this has been a very active area of research. The initial conjecture of Linnik [10] predicts cancellations when the coefficients m

2010 *Mathematics Subject Classification.* 11L05, 11T23.

Key words and phrases. Kloosterman sums, Prime powers.

and n are fixed but the modulus q varies, see [13] for results towards a uniform version of this conjecture.

The dual question, concerning cancellations between Kloosterman sums $\mathcal{K}(m, n; q)$ modulo the same integer q but with varying coefficients m and n when one of both runs through a consecutive interval, see [4, 12, 14] and references therein. Questions of this type usually become much harder when one imposes arithmetic conditions on the parameters, such as square-freeness, smoothness or primality. In this direction, in the case of prime moduli $q = p$, Blomer, Fouvry, Kowalski, Michel and Milićević [2] have shown the existence of nontrivial cancellations between the Kloosterman sums $\mathcal{K}(\ell, a; p)$ when ℓ runs over primes up to some parameter $X \geq q^{3/4+\varepsilon}$ for any fixed $\varepsilon > 0$ (with the goal to have X as small as possible compared to q).

In this paper, using a different technique, we obtain analogues of these results in the case where $q = p^k$ is a power of an odd prime p for some sufficiently large integer k , which in fact allows us to reduce the amount of averaging $X \geq q^\varepsilon$ for any fixed $\varepsilon > 0$.

As in [2], our approach is based on bounding certain bilinear sums of Kloosterman sums. Namely, given two sequences of weights $\mathcal{A} = \{\alpha_m\}_{m=1}^M$ and $\mathcal{B} = \{\beta_n\}_{n=1}^N$ with

$$\max_{m=1,\dots,M} |\alpha_m| \leq 1 \quad \text{and} \quad \max_{n=1,\dots,N} |\beta_n| \leq 1,$$

we consider the bilinear sums

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) = \sum_{m=1}^M \sum_{n=1}^N \alpha_m \beta_n \mathcal{K}(mn, a; q).$$

Recently a series of bounds has been obtained, by various methods, on the sum $S_{a,q}(\mathcal{A}, \mathcal{B}; M, N)$ when $q = p$ is prime, see [1, 2, 8, 15, 16] and references therein. Here, using a different technique, we obtain analogues of these results in the case where $q = p^k$ is a large power of an odd prime p . We believe this bound can be of independent interest and may find some other applications.

1.2. Main results. Before we formulate our results we need to recall that the notations $U \ll V$ and $U = O(V)$, are equivalent to $|U| \leq cV$ for some constant $c > 0$. We note that we do not number implicit constants, which we usually also denote by c so they are allowed to change their values in different statements.

We write \ll_ρ and O_ρ to indicate that this constant may depend on the parameter ρ .

Theorem 1.1. *Let $q = p^k$, $k \in \mathbb{Z}$ be a power of an odd prime p . Then for any fixed constant $0 < \lambda < 1$ and $q^\lambda < M, N < q$, there exist a constant $H_1(\lambda) > 0$ depending only on λ and an absolute constant $c > 0$ such that for any $k > H_1(\lambda)$ and $\tau(\lambda) = c\lambda^3$ we have*

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) \ll_\lambda MNq^{-\tau(\lambda)},$$

uniformly over odd primes p and integers a with $\gcd(a, p) = 1$, where the implied constant depends only on λ .

We note that for some applications one also need to restrict the summation to a hyperbolic domain.

Corollary 1.2. *Let $q = p^k$, $k \in \mathbb{Z}$ be a power of an odd prime p . Then for any fixed constant $0 < \lambda < 1$ and $q^\lambda < U, V < X$ with $X < q$, there exist a constant $H_2(\lambda) > 0$ depending only on λ and an absolute constant $c > 0$ such that for any $k > H_2(\lambda)$ and $\vartheta(\lambda) = c\lambda^3$ we have*

$$\sum_{\substack{m \geq U, n \geq V \\ mn \leq X}} \alpha_m \beta_n \mathcal{K}(mn, a; q) \ll_\lambda Xq^{-\vartheta(\lambda)},$$

uniformly over odd primes p and integers a with $\gcd(a, p) = 1$, where the implied constant depends only on λ .

We use Corollary 1.2 in a combination with the main result of [11] to derive:

Theorem 1.3. *Let $q = p^k$, $k \in \mathbb{Z}$ be a power of an odd prime p and $q^\varepsilon < X \leq q$. Then there exist a constant $H_3(\varepsilon) > 0$ depending only on λ and an absolute constant $c > 0$ such that for any $k > H_3(\varepsilon)$ and $\delta(\varepsilon) = c\varepsilon^3$ we have*

$$\sum_{\substack{\ell \leq X \\ \ell \text{ prime}}} \mathcal{K}(\ell, a; q) \ll_\varepsilon Xq^{-\delta(\varepsilon)}$$

uniformly over odd primes p and integers a with $\gcd(a, p) = 1$, where the implied constant depends only on ε .

2. PRELIMINARIES

2.1. Some bounds on Kloosterman sums. Let $\Re z$ denote the real part of a complex number z .

First we record the following explicit formula, see, for example, [5, Equation (12.39)].

Lemma 2.1. *Let $q = p^k$ with p being an odd prime and $k \geq 2$, $k \in \mathbb{Z}$. Then for $\gcd(a, q) = 1$ we have*

$$\mathcal{K}(n, a; q) = \begin{cases} 2 \left(\frac{r}{p}\right)^k \Re \vartheta_q e\left(\frac{2r}{q}\right), & \text{if } \left(\frac{na}{p}\right) = 1, \\ 0, & \text{if } \left(\frac{na}{p}\right) = -1, \end{cases}$$

where r is a solution of $r^2 \equiv na \pmod{q}$, $\left(\frac{r}{p}\right)$ is the Legendre symbol, ϑ_q equals 1 if $q \equiv 1 \pmod{4}$ and i if $q \equiv 3 \pmod{4}$.

Easy calculations show the following well-know fact (see also [11]):

Lemma 2.2. *Let p be an odd prime and $k \geq 2$ be a positive integer. If $\gcd(a, p) = 1$ and $p \mid n$, then the Kloosterman sums $\mathcal{K}(n, a; p^k) = 0$.*

One of our principal technical tools is the following estimate from [11] on the cancellations amongst Kloosterman sums,

Lemma 2.3. *Let $q = p^k$, $k \in \mathbb{Z}$ be a power of an odd prime p . Then for any fixed constant $0 < \lambda < 1$ and $q^\lambda < N < q$, there exist a constant $K_0(\lambda)$ depending only on λ and an absolute constant $c > 0$ such that for any $k > K_0(\lambda)$ and $\tau(\lambda) = c\lambda^3$ we have*

$$\sum_{1 \leq n \leq N} \mathcal{K}(n, a; q) \ll_\lambda N q^{-\tau(\lambda)}$$

uniformly over odd primes p and integers a with $\gcd(a, p) = 1$, where the implied constant depends only on λ .

2.2. Short exponential sums with special polynomials. The following bound is contained in the proof of [11, Theorem 1.2] (and in fact is in the core of this proof).

Lemma 2.4. *Suppose $\gcd(h, q) = 1$, $q = p^k$ with p an odd prime and $k \in \mathbb{Z}$. For $q^\eta < N < q$ with $0 < \eta < 1$ being a fixed constant, there exists a constant $k_0(\eta) > 0$, such that for the polynomial by*

$$(2.1) \quad f(X) = \sum_{j=0}^{\lfloor k/s \rfloor} g(j) \gamma^j p^{js} X^j,$$

where γ is an arbitrary integer with $\gcd(\gamma, p) = 1$,

$$s = \left\lfloor \frac{\eta \log N}{3000 \log p} \right\rfloor,$$

$g(0) = 1$ and $g(j)$ with $1 \leq j \leq \lfloor k/s \rfloor$ are integers given by

$$g(j) \equiv \frac{1/2(1/2 - 1) \cdots (1/2 - j + 1)}{j!} \pmod{p^k}, \quad 0 \leq g(j) < p^k,$$

and any $k > k_0(\eta)$, we have

$$\sum_{n \leq N} e\left(\frac{hf(n)}{q}\right) \ll_{\eta} Nq^{-\rho(\eta)},$$

where $\rho(\eta) = c\eta^3$ with some absolute constant $c > 0$ and the implied constant depends only on η .

2.3. Vaughan identity. As usual, we use $\Lambda(n)$ to denote the von Mangoldt function

$$\Lambda(n) = \begin{cases} \log \ell & \text{if } n \text{ is a power of a prime } \ell, \\ 0 & \text{otherwise.} \end{cases}$$

We use the following result of Vaughan [17] in the form given by Davenport [3, Chapter 24].

Lemma 2.5. *For any complex-valued function $f(n)$ and any real numbers $1 < U, V \leq X$, we have*

$$\sum_{n \leq X} \Lambda(n)f(n) \ll \Sigma_1 + \Sigma_2 \log(UV) + \Sigma_3 \log X + |\Sigma_4|,$$

where

$$\begin{aligned} \Sigma_1 &= \left| \sum_{n \leq U} \Lambda(n)f(n) \right|, \\ \Sigma_2 &= \sum_{v \leq UV} \left| \sum_{s \leq N/v} f(sv) \right|, \\ \Sigma_3 &= \sum_{v \leq V} \max_{w \geq 1} \left| \sum_{w \leq s \leq N/v} f(sv) \right| \end{aligned}$$

and

$$\Sigma_4 = \sum_{\substack{uv \leq X \\ u > U, v > V}} \Lambda(u) \left(\sum_{d|v, d \leq V} \mu(d) \right) f(uv).$$

3. PROOF OF MAIN RESULTS

3.1. Proof of Theorem 1.1. Note that due to the symmetry of the sum and the claimed bound with respect to M and N , we can always assume that $M \geq N$.

Let $1 \leq s \leq k$ be a parameter to be determined. Write

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) = \sum_{u=1}^{p^s} \sum_{v=1}^{p^s} \sum_{\substack{m \leq M \\ m \equiv u \pmod{p^s}}} \sum_{\substack{n \leq N \\ n \equiv v \pmod{p^s}}} \alpha_m \beta_n \mathcal{K}(mn, a; q).$$

Then by Lemma 2.2, we have

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) \leq \sum_{u=1}^{p^s} \sum_{v=1}^{p^s} \sum_{\substack{n \leq N \\ n \equiv v \pmod{p^s}}} \left| \sum_{\substack{m \leq M \\ m \equiv u \pmod{p^s}}} \alpha_m \mathcal{K}(mn, a; q) \right|.$$

Now by Lemma 2.1, we get

$$\begin{aligned} & S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) \\ & \leq 2 \sum_{u=1}^{p^s} \sum_{v=1}^{p^s} \sum_{\substack{n \leq N \\ n \equiv v \pmod{p^s}}} \left| \sum_{\substack{m \leq M \\ m \equiv u \pmod{p^s} \\ \left(\frac{amn}{p}\right)=1}} \alpha_m \left(\frac{r_{m,n}}{p}\right)^k \Re \vartheta_q e\left(\frac{2r_{m,n}}{q}\right) \right|, \end{aligned}$$

where $r_{m,n}$ is a solution to $r_{m,n}^2 \equiv amn \pmod{q}$ (the inequality holds for any choice of this solution). Thus

$$(3.1) \quad S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) \leq 2 \sum_{u=1}^{p^s} \sum_{\substack{v=1 \\ \left(\frac{auv}{p}\right)=1}}^{p^s} T_s(u, v),$$

where

$$(3.2) \quad T_s(u, v) = \sum_{\substack{n \leq N \\ n \equiv v \pmod{p^s}}} \left| \sum_{\substack{m \leq M \\ m \equiv u \pmod{p^s}}} \alpha_m \left(\frac{r_{m,n}}{p}\right)^k \Re \vartheta_q e\left(\frac{2r_{m,n}}{q}\right) \right|.$$

Note that $r_{m,n}^2 \equiv amn \equiv auv \pmod{p}$, thus the Legendre symbol $\left(\frac{r_{m,n}}{p}\right)$ does not depend on m and n . We now use the Cauchy inequality and derive

$$T_s(u, v)^2 \ll (Np^{-s} + 1) \sum_{\substack{m_1, m_2 \leq M \\ m_1 \equiv u \pmod{p^s} \\ m_2 \equiv u \pmod{p^s}}} \left| \sum_{\substack{n \leq N \\ n \equiv v \pmod{p^s}}} e\left(\frac{2(r_{m_1,n} - r_{m_2,n})}{q}\right) \right|,$$

with $r_{m_i,n}$ being a solution of the congruence $r^2 \equiv m_i n a \pmod{q}$ for $i = 1, 2$.

Now we consider the inner sum over n . Note that for $i = 1, 2$, we have $\gcd(am_i, q) = 1$, then we use the following argument, which is similar to that in [6] and [11].

By $n \equiv v \pmod{p^s}$, there exists $t \in \mathbb{Z}$, such that $n = v + p^s t$. Now we have

$$r_{m_i,n}^2 \equiv am_i(v + p^s t) \equiv am_i v(1 + \bar{v} p^s t) \pmod{q},$$

with $v\bar{v} \equiv 1 \pmod{q}$. Note that $am_i v \equiv auv \pmod{p}$, then

$$\left(\frac{am_i v}{p} \right) = 1.$$

By the *Hensel lifting*, there exists an integer ω , such that $0 \leq \omega < p^s$ and

$$\omega^2 \equiv auv \pmod{p^s},$$

and also for each m_i there exists an integer ω_{m_i} such that

$$\omega_{m_i}^2 \equiv am_i v \pmod{q}$$

and $\omega_{m_i} \equiv \omega \pmod{p^s}$ for $i = 1, 2$. Thus

$$r_{m_i,n}^2 \equiv am_i v \equiv \omega_{m_i}^2 (1 + \bar{v} p^s t) \pmod{q}.$$

We remark that ω_{m_i} is determined by a , m_i and v , and does not depend on n . Consider $1 + \bar{v} p^s t$ in the p -adic field \mathbb{Q}_p . By the Taylor expansion (see [7, Chapter IV.1]), we have

$$(1 + \bar{v} p^s t)^{1/2} = 1 + \sum_{j=1}^{\infty} \binom{1/2}{j} \bar{v}^j p^{js} t^j$$

for $s \geq 1$ with the coefficients

$$\binom{1/2}{j} = \frac{1/2(1/2-1) \cdots (1/2-j+1)}{j!}, \quad j = 1, 2, \dots,$$

which are p -adic integers, since p is an odd prime. Then we have

$$(1 + \bar{v} p^s t)^{1/2} \equiv 1 + \sum_{j=1}^{\lfloor k/s \rfloor} g(j) \bar{v}^j p^{js} t^j \pmod{p^k},$$

where $g(j)$ with $1 \leq j \leq \lfloor k/s \rfloor$ are integers given by

$$(3.3) \quad g(j) \equiv \binom{1/2}{j} \pmod{p^k}, \quad 0 \leq g(j) < p^k.$$

Thus we get two solutions for the quadratic congruence of $r_{m_i,n}$ in the inner sum in (3.2).

$$r_{m_i,n} \equiv \pm \omega_{m_i} f(t) \pmod{q},$$

where the polynomial $f(X)$ is given by (2.1) as in Lemma 2.4 with $\gamma = \bar{v}$.

Choosing the solution $r_{m_i,n} \equiv \omega_{m_i} f(t) \pmod{q}$, then we have

$$T_s(u, v)^2 \leq (Np^{-s} + 1) \sum_{\substack{m_1, m_2 \leq M \\ m_1 \equiv u \pmod{p^s} \\ m_2 \equiv u \pmod{p^s}}} \left| \sum_{t \leq (N-v)/p^s} e \left(\frac{2(\omega_{m_1} - \omega_{m_2})f(t)}{q} \right) \right|.$$

Since $v \leq p^s$, we can replace the range of t by $t \leq N/p^s$ up to a small error term and thus we get

$$(3.4) \quad T_s(u, v)^2 \ll (Np^{-s} + 1) \sum_{\substack{m_1, m_2 \leq M \\ m_1 \equiv u \pmod{p^s} \\ m_2 \equiv u \pmod{p^s}}} \left| \sum_{t \leq N/p^s} e \left(\frac{2(\omega_{m_1} - \omega_{m_2})f(t)}{q} \right) \right| \\ + (Np^{-s} + 1)(Mp^{-s} + 1)^2.$$

We now choose

$$(3.5) \quad B(\lambda) = 3000/\lambda > 3000 \quad \text{and} \quad s = \left\lfloor \frac{\log N}{B(\lambda) \log p} \right\rfloor.$$

Since $q^\lambda < N \leq M < q = p^k$, then we have $s \leq k/B(\lambda)$. Hence,

$$(3.6) \quad N/p^s \geq q^{\lambda/2} \quad \text{and} \quad k - 3s > k/2.$$

In particular we see from (3.6) that

$$Mp^{-s} + 1 \ll Mp^{-s} \quad \text{and} \quad Np^{-s} + 1 \ll Np^{-s}.$$

Thus (3.4) can be simplified as

$$(3.7) \quad T_s(u, v)^2 \ll Np^{-s} \sum_{\substack{m_1, m_2 \leq M \\ m_1 \equiv u \pmod{p^s} \\ m_2 \equiv u \pmod{p^s}}} \left| \sum_{t \leq N/p^s} e \left(\frac{2(\omega_{m_1} - \omega_{m_2})f(t)}{q} \right) \right| \\ + M^2 Np^{-3s}.$$

Let $\text{ord}_p(n)$ denote the p -adic order of integer n . For a fixed m_1 , we claim that

$$\# \{m_2 \leq M : m_2 \equiv m_1 \pmod{p^s}, \text{ord}_p(\omega_{m_1} - \omega_{m_2}) \geq 3s\} \leq Mp^{-3s} + 1.$$

To see this, we note that $\text{ord}_p(\omega_{m_1} - \omega_{m_2}) \geq 3s$ implies

$$\omega_{m_1}^2 \equiv \omega_{m_2}^2 \pmod{p^{3s}}.$$

Since $\gcd(av, q) = 1$, then by the definition of ω_{m_i} , we have the congruence $m_2 \equiv m_1 \pmod{p^{3s}}$, which yields our claim.

We estimate the contribution of this case to $T_s(u, v)^2$ trivially as

$$Np^{-s} \sum_{\substack{m_1 \leq M \\ m_1 \equiv u \pmod{p^s}}} \sum_{\substack{m_2 \leq M \\ m_2 \equiv m_1 \pmod{p^s} \\ \text{ord}_p(\omega_{m_1} - \omega_{m_2}) \geq 3s}} \sum_{t \leq N/p^s} 1 \ll MN^2 p^{-3s} (Mp^{-3s} + 1).$$

Hence, we only need to estimate the exponential sum

$$\sum_{t \leq N/p^s} e \left(\frac{2(\omega_{m_1} - \omega_{m_2})f(t)}{q} \right),$$

with $\text{ord}_p(\omega_{m_1} - \omega_{m_2}) < 3s$. After cancelling the factor p^s , we can get a similar exponential sum of the type

$$\sum_{t \leq N/p^s} e \left(\frac{hf(t)}{p^r} \right)$$

with $\gcd(h, q) = 1$ and $r > k - 3s$. To bound this sum, we recall our choice (3.5) and apply Lemma 2.4 and get

$$\sum_{t \leq N/p^s} e \left(\frac{2(\omega_{m_1} - \omega_{m_2})f(t)}{q} \right) \ll Np^{-s} q^{-\rho(\lambda/2)},$$

for $k \geq k_0(\lambda/2)$, where k_0 and ρ are the same as in Lemma 2.4. Insert this bound to (3.7), we get

$$\begin{aligned} T_s(u, v)^2 &\ll M^2 N^2 p^{-4s} q^{-\rho(\lambda/2)} + MN^2 p^{-3s} (Mp^{-3s} + 1) + M^2 N p^{-3s} \\ &= M^2 N^2 p^{-4s} q^{-\rho(\lambda/2)} + M^2 N^2 p^{-6s} + M^2 N p^{-3s}. \end{aligned}$$

Then we have

$$T_s(u, v) \ll MN p^{-2s} q^{-\rho(\lambda/2)/2} + MN p^{-3s} + MN^{1/2} p^{-3s/2},$$

which after the substitution in (3.1) yields

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) \ll MN q^{-\rho(\lambda/2)/2} + MN^{1/2} p^{s/2} + MN p^{-s}.$$

Note that the definition of s implies that

$$\begin{aligned} s &\geq \frac{\log N}{B(\lambda) \log p} - 1 = \frac{\lambda \log N}{3000 \log p} - 1 \\ &= \frac{\lambda k \log N}{3000 \log q} - 1 \geq \frac{\lambda k \log N}{6000 \log q} = \frac{\log N}{2B(\lambda) \log p}, \end{aligned}$$

provided that k is large enough (we also recall that $q > M \geq N > q^\lambda$). Hence

$$N^{1/(2B(\lambda))} \leq p^s \leq N^{1/B(\lambda)},$$

from which the result follows.

3.2. Proof of Corollary 1.2. Separating the summation over m in dyadic ranges and slightly reducing the constant c in the definition of $\vartheta(\lambda)$, it is enough to show that for any M_1, M_2 with

$$M_2 \leq 2M_1 \quad \text{and} \quad U \leq M_1 < M_2 \leq 2X/V,$$

we have

$$(3.8) \quad \sum_{m=M_1}^{M_2} \sum_{V \leq n \leq X/m} \alpha_m \beta_n \mathcal{K}(mn, a; q) \ll_\lambda X q^{-\vartheta(\lambda)}.$$

Let $L = \lfloor X/M_1 \rfloor$. Clearly we can assume that $L \geq V$ as otherwise the sum over n is void and there is nothing to prove. In particular, we can assume that

$$L \geq q^\lambda.$$

By the orthogonality of exponential functions, we write

$$\begin{aligned} & \sum_{m=M_1}^{M_2} \sum_{V \leq n \leq X/m} \alpha_m \beta_n \mathcal{K}(mn, a; q) \\ &= \sum_{m=M_1}^{M_2} \sum_{V \leq n \leq L} \frac{1}{L} \sum_{z=0}^{L-1} \sum_{w=0}^{X/m} e(z(w-n)/L) \alpha_m \beta_n \mathcal{K}(mn, a; q) \\ &= \frac{1}{L} \sum_{z=0}^{L-1} \sum_{m=M_1}^{M_2} \sum_{w=0}^{X/m} e(zw/L) \sum_{V \leq n \leq L} \alpha_m \beta_n e(-zn/L) \mathcal{K}(mn, a; q). \end{aligned}$$

Using that for $z = 0, \dots, L-1$ we have

$$\sum_{w=0}^{X/m} e(zw/L) \ll \frac{L}{1 + \min\{z, L-z\}},$$

see [5, Bound (8.6)]. We now derive

$$\begin{aligned} & \sum_{m=M_1}^{M_2} \sum_{V \leq n \leq X/m} \alpha_m \beta_n \mathcal{K}(mn, a; q) \\ (3.9) \quad &= \sum_{z=0}^{L-1} \frac{1}{1 + \min\{z, L-z\}} \sum_{m=M_1}^{M_2} \sum_{V \leq n \leq L} \tilde{\alpha}_{z,m} \tilde{\beta}_{z,n} \mathcal{K}(mn, a; q) \end{aligned}$$

with some weights $|\tilde{\alpha}_{z,m}| \leq 1$ and $|\tilde{\beta}_{z,n}| \leq 1$ (in particular $\tilde{\beta}_{z,n} = \beta_n e(-zn/L)$). Thus, by Theorem 1.1 for every $z = 0, \dots, L-1$, for the double sum over m and n we have the bound

$$\sum_{m=M_1}^{M_2} \sum_{V \leq n \leq L} \tilde{\alpha}_{z,m} \tilde{\beta}_{z,n} \mathcal{K}(mn, a; q) \ll M_2 L q^{-\tau(\lambda)} \ll X q^{-\tau(\lambda)},$$

which after substitution in (3.9) implies (3.8) and concludes the proof.

3.3. Proof of Theorem 1.3. Using partial summation, one can easily see that it is enough to estimate the sum

$$\tilde{S}(X; a, q) = \sum_{n \leq X} \Lambda(n) \mathcal{K}(n, a; q).$$

We now apply Lemma 2.5 (with $f(n) = \mathcal{K}(n, a; q)$) where we take $U = V = X^{1/3}$, for which we need to estimate the sums:

$$\begin{aligned} \Sigma_1 &= \left| \sum_{n \leq U} \Lambda(n) \mathcal{K}(n, a; q) \right|, \\ \Sigma_2 &= \sum_{v \leq UV} \left| \sum_{s \leq X/v} \mathcal{K}(sv, a; q) \right|, \\ \Sigma_3 &= \sum_{v \leq V} \max_{w \geq 1} \left| \sum_{w \leq s \leq X/v} \mathcal{K}(sv, a; q) \right| \end{aligned}$$

and

$$\Sigma_4 = \sum_{\substack{uv \leq X \\ u > U, v > V}} \Lambda(u) \left(\sum_{d|v, d \leq V} \mu(d) \right) \mathcal{K}(uv, a; q).$$

Using the Weil bound (1.1), or its more precise version given in Lemma 2.1, we have

$$\Sigma_1 \ll_{\varepsilon} X^{1/3} q^{\varepsilon/3} < X q^{-\varepsilon/3}.$$

For Σ_2 , note that $v \leq UV = X^{2/3}$, then $X/v \geq X^{1/3} > q^{\varepsilon/3}$. Now Lemma 2.3 can be applied to the sum over s . Hence there exist constants $K_1(\varepsilon) > 0$ and $\tau_1(\varepsilon) > 0$ such that

$$\Sigma_2 \ll_{\varepsilon} X q^{-\tau_1(\varepsilon)}$$

holds uniformly for any odd prime p and $k > K_1(\varepsilon)$.

For Σ_3 , write the inner sum over s into

$$(3.10) \quad \sum_{w \leq s \leq X/v} \mathcal{K}(sv, a; q) = \sum_{s \leq X/v} \mathcal{K}(sv, a; q) - \sum_{s < w} \mathcal{K}(sv, a; q).$$

The contribution of the first sum on the right side can be bounded similarly as Σ_2 . For the contribution of the second sum, If $w < q^{\varepsilon/4}$, then by the Weil bound we have

$$\sum_{s \leq w} \mathcal{K}(sv, a; q) \ll_{\varepsilon} q^{\varepsilon/3}.$$

If $w \geq q^{\varepsilon/4}$, then Lemma 2.3 can be applied to the above sum. It follows from the above treatment that there exist constants $K_2(\varepsilon) > 0$ and $\tau_2(\varepsilon) > 0$ such that

$$\Sigma_3 \ll_{\varepsilon} X q^{-\tau_2(\varepsilon)}$$

holds uniformly for any odd prime p and $k > K_2(\varepsilon)$.

For Σ_4 , by Corollary 1.2 there exist constants $K_3(\varepsilon) > 0$ and $\tau_3(\varepsilon) > 0$ such that

$$\Sigma_4 \ll_{\varepsilon} X q^{-\tau_3(\varepsilon)}$$

holds uniformly for any odd prime p and $k > K_3(\varepsilon)$. It is also easy to see that for the functions $\tau_{\nu}(\varepsilon)$ we can take $\tau_{\nu}(\varepsilon) = c_{\nu} \varepsilon^3$ for some absolute constants $c_{\nu} > 0$, for every $\nu = 1, 2, 3$.

Now the desired bound on $\tilde{S}(X; a, q)$ and thus Theorem 1.3 follow from the above estimates.

REFERENCES

- [1] V. Blomer, É. Fouvry, E. Kowalski, P. Michel and D. Milićević, ‘On moments of twisted L -functions’, *Amer. J. of Math.*, (to appear).
- [2] V. Blomer, É. Fouvry, E. Kowalski, P. Michel and D. Milićević, ‘Some applications of smooth bilinear forms with Kloosterman sums’, *Proc. Steklov Math. Inst.*, (to appear).
- [3] H. Davenport, *Multiplicative number theory*, 2nd ed., Springer-Verlag, New York, 1980.
- [4] É. Fouvry, P. Michel, J. Rivat and A. Sárközy, ‘On the pseudorandomness of the signs of Kloosterman sums’, *J. Aust. Math. Soc.*, **77** (2004), 425–436.
- [5] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.
- [6] R. Khan, ‘The divisor function in arithmetic progressions modulo prime powers’, *Mathematika*, **62** (2016), 898–908.
- [7] N. Koblitz, *p -adic numbers, p -adic analysis, and zeta-functions*, Second edition, Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984.

- [8] E. Kowalski, P. Michel and W. Sawin, ‘Bilinear forms with Kloosterman sums and applications’, *Preprint*, 2015 (available from <http://arxiv.org/abs/1511.01636>).
- [9] N. V. Kuznetsov, ‘The Petersson conjecture for cusp forms of weight zero and the Linnik conjecture. Sums of Kloosterman sums’, *Math. USSR-Sb.*, **39** (1981), 299–342.
- [10] Y. V. Linnik, ‘Additive problems and eigenvalues of the modular operators,’ *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, Inst. Mittag-Leffler, Djursholm, 1963, 270–284.
- [11] K. Liu, I. E. Shparlinski and T. P. Zhang, ‘Divisor problem in arithmetic progressions modulo a prime power’, *Preprint*, 2016 (available from <http://arxiv.org/abs/1602.03583>).
- [12] H. Niederreiter, ‘The distribution of values of Kloosterman sums’, *Arch. Math.*, **56** (1991), 270–277.
- [13] P. Sarnak and J. Tsimmerman, ‘On Linnik and Selberg’s conjecture about sums of Kloosterman sums’, *Algebra, Arithmetic, and Geometry: in Honor of Yu. I. Manin, Vol. II*, Progress in Mathematics v.270, Birkhäuser, Boston, MA, 2009, 619–635.
- [14] I. E. Shparlinski, ‘Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average’, *Michigan Math. J.*, **56** (2008), 99–111.
- [15] I. E. Shparlinski, ‘Bilinear forms with Kloosterman and Gauss sums’, *Preprint*, 2016 (available from <http://arxiv.org/abs/1608.06160>).
- [16] I. E. Shparlinski and T. P. Zhang, ‘Cancellations amongst Kloosterman sums’, *Acta Arith.*, **176** (2016), 201–210.
- [17] R. C. Vaughan, ‘An elementary method in prime number theory’, *Acta Arith.*, **37** (1980), 111–115.

SCHOOL OF MATHEMATICS AND STATISTICS, QINGDAO UNIVERSITY, No.308,
 NINGXIA ROAD, SHINAN, QINGDAO, SHANDONG, 266071, P. R. CHINA
E-mail address: liukui@qdu.edu.cn

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,
 SYDNEY, NSW 2052, AUSTRALIA
E-mail address: igor.shparlinski@unsw.edu.au

SCHOOL OF MATHEMATICS AND INFORMATION SCIENCE, SHAANXI NORMAL
 UNIVERSITY, XI’AN 710119 SHAANXI, P. R. CHINA
E-mail address: tpzhang@snnu.edu.cn